Technologies for Secure RFID Authentication of Medicinal Pills and Capsules

L. Richard Carley, Gurkan Colak, Louis Chomas, Larry Pileggi and Kenneth Mai
Department of Electrical and Computer Engineering
Carnegie Mellon University
Pittsburgh, USA
carley@ece.cmu.edu

***Abstract*—This paper addresses the problem of counterfeiting of medicines in the form of pills and capsules by proposing a novel micron-scale secure RFID tag that would be inserted into the pill or capsule during the manufacturing process. For secure identification and authentication, a tagged pill or capsule would be scanned by a small inexpensive RFID reader, and key medicine information such as the drug type, manufacturer, and expiration date would be retrieved from a secure database. This application is enabled by an RFID tag integrated circuit (IC) incorporating an on-chip ID storage and custom security engine with a novel on-chip antenna (OCA) structure that has the potential to achieve an order of magnitude greater working distance at constant power level when compared to prior art passive single-chip silicon RFID tags with OCAs. This paper describes the proposed solution in detail and presents analysis, electromagnetic simulation, and circuit simulation results supporting its design and performance.**

Keywords—RFID; passive RFID; Counterfeit medicines; wireless power delivery; AES encryption; on-chip antenna (OCA); MEMS post-processing.

I. INTRODUCTION

The need to prevent counterfeit drugs from being introduced into the legitimate supply chain is acute. The World Health Organization has estimated that counterfeit drugs represent more than 10 percent of global sales, and that they are responsible for thousands of deaths each year [11]. One possible solution that has been proposed for this problem is the use of radio-frequency ID (RFID) tags. To date, the size and cost of today's RFID tags has limited their application to drug packaging. However, as Novartis's James Christian, CSO of the $37 billion company based in Basel, Switzerland, noted "we have had experience with counterfeit product in genuine packaging, and genuine product in counterfeit packaging" [11]. Pharmaceutical products are routinely and legally repackaged in both the United States and the European Union. "If a pharmaceutical company invests a great deal of money into putting security devices in packaging, the product could easily be transferred legally to a package with no security device," Christian says [11]. "And now someone has a collection of genuine packaging with security devices that they might throw away or use in another manner."

The second problem, Christian notes, is that an enterprising drug counterfeiter with the appropriate RFID code reader, can simply read the code from the RFIDs on valid packaging and program their own RFIDs to mimic valid codes. Moreover, even when drugs are from a valid manufacturer, they may be beyond their expiration date. Today, the only approach to handle date validity is the data stamp on the package, which creates opportunity for drug counterfeiters to buy up out-of-date drugs, repackaging them with modified expiration dates.

It is difficult to estimate the cost of people using invalid medicines, out-of-date-code mediciness, or even just incorrect medicines; however, the cost is likely to be extremely high. Therefore, it is important to develop a technological solution to this societal concern. In this paper we describe a set of technologies that enable ultra-low-cost secure RFID tagging of individual medicinal pills and capsules. The key innovation making this possible is the development of a novel on-chip antenna (OCA) for passive silicon RFID tags that achieves an order of magnitude more range than prior art approaches, while also fitting on a chip that is sized to be harmlessly ingested by humans (e.g., < 1mm x 1mm [4]).

The secure RFID solution proposed in this paper consists of three parts: a secure passive RFID Tag with OCA incorporated into the pill or capsule, an RFID Reader connected to the internet, and computation/database infrastructure in the cloud that provides authentication. The goal is to created a system in which the manufacturer and the expiration date of RFID tagged medicines can be securely validated at any time using small, portable RFID readers with an internet connection. Ideally, secure validation can be done in pharmacies, hospitals, clinics, elderly care facilities, and even in one's own home.

This paper starts by providing some background on prior research work on single-chip silicon RFID tags with OCAs and then reviews the key requirements that must be met by any proposed RFID tag for individual medicinal pills and capsules. Next, the paper describes the technological building blocks that together form a viable RFID solution for this problem. We then provide detailed E&M and circuit simulation results for a specific set of design parameters that are selected to best address the key requirements. Lastly, we provide conclusions.

II. BACKGROUND

The idea of building a complete RFID tag on a small integrated circuit substrate has been pursued for many years. A review of single-chip silicon RFID tags with OCAs can be

We acknowledge partial financial support for this research from the Disruptive Health Technology Institute, a partnership between Highmark and Carnegie Mellon University.

found in Scherjon [9]. Several examples of research on silicon RFID tags incorporating OCAs are found in [1]–[3][10]12]. At 13.56-MHz frequency, Abrial et al. [1] reported a passive silicon RFID tag with OCA fabricated on a 4mm x 4mm 0.25μm CMOS IC. However, this design only operated with the RFID reader and the RFID tag nearly in contact (e.g., under 3mm spacing) and the die is much larger than the size required for this application. Usami [2] presented a Hitachi OCA RFID chip operating at 2.45GHz with an area of just 0.4mm x 0.4mm, fabricated using a gold-plating method to build the OCA directly on top of the silicon substrate. However, only extremely short range operation was possible. Chen et al. [3] improved OCA efficiency by using microelectromechanical system (MEMS) post-processing techniques to add a 15μm thick oxide layer on top of a 0.5mm x 1mm 0.13μm CMOS IC. Even so, the maximum allowable spacing between the RFID reader and tag was only 0.5mm [3]. For comparison, in the pill authentification scenario, the RFID reader and tag spacing must be 5-10mm (>10X more than that achieved in [3]).

Jingtian et al. [10] fabricated a 1mm x 1mm 0.18μm CMOS RFID tag with an OCA that operated at up to 10mm separation by utilizing advanced CMOS rectifiers and extremely low tag power dissipation – much lower than that required for the secure pill authentication. And Radiom et al. [12] demonstrated a 4.4mm x 1.5mm 0.13μm CMOS RFID tag with an OCA that operated at up to 400mm reader-to-tag spacing; but, it could only delivered sub-μW power levels.

The primary challenge is that the RF power that can be harvested is extremely low because the area of an OCA is extremely small, which reduces the power transfer between the tag and reader antennas. In addition, the proximity of the tag antenna to the low resistance substrate of a typical silicon integrated circuit (IC) greately reduces the RF energy received at a planar antenna built on top of an IC substrate. It is this poor power transfer that limits the maximum allowable spacing between the RFID reader and the RFID tag in the proposed application.

III. Key Design Requirements

RFID technology for pill authentication must satisfy a number of challenging requirements. These requirements can be broken down into three categories; safety, effectiveness, and cost. In this section, we review these key design requirements.

A. Safety

The simplest way for an RFID tag to uniquely identify an individual pill or capsule as being from a particular manufacturer and as being within date code, is for the RFID tag to be embedded within the pill or capsule. This also makes removing the RFID tag and transfering it to another (presumably counterfeit) pill nearly impossible. The biggest safety issue in this scenario is that the RFID tag must pass through the human digestive tract without causing any harm. There are two aspects to this – size and chemical composition. The smaller the volume of the RFID tag, and the smaller the largest dimension of the RFID tag, the less likely it is to cause an issue within the human digestive system. The US Food and Drug Administration has already approved the incorporation of a 1mm x 1mm Si IC substrate into medicinal pills and capsules [4]. Therefore, we target a single-chip RFID solution that is smaller than 1mm x 1mm. Since it is difficult to create a biologically safe battery this small, we focus on passive RFID tags.

The second safety issue is that the surface of the RFID tag will be attacked by acids in the human digestive system, which may cause some of the compounds on the surface of the RFID tag to be "digested" and to enter the blood stream. In order to insure that the RFID tag will not cause any contamination as it passes through the digestive tract, its entire surface should be coated with inert substances; e.g., silicon and silicon nitride.

B. Effectiveness

The primary goal of the proposed RFID solution is to significantly reduce counterfeiting of medicines. In order to achieve this goal, the proposed solution must address a number of different approaches to counterfeiting. At the simplest level, we could insert an RFID tag into pills that simply responded with a unique manufacturer ID code and an expiration date when interrogated by the RFID reader. This scenario has the advantage of simplicity, but there are many ways in which it could be circumvented. For example, counterfeiters could also counterfeit the RFID tags. Once the design of the RFID tags is commoditized and standardized, there will be a number of manufacturers capable of fabricating them around the world. Since the ID of the original phamaceutical company can be read from any pill or capsule they manufacture, it is easy for the counterfeiter to specify that ID when ordering RFID tags. While governments could legally require manufacturers to validate that the ID and the company ordering the RFID tags match, it could be difficult to enforce such a rule. And, this scenario still cannot be used to keep people from taking the wrong medicines from the same manufacturer.

A technological approach is adopted in this paper to prevent such counterfeiting by providing each pill or capsule with a unique ID. In this solution RFID tags incorporate write-once memory and a secure authentication engine. The RFID tags would be written with a unique secure ID code by the pharmaceutical company right before or after they are inserted into the pill or capsule; and, that unique ID would be saved to a secure database. And, by using a sufficiently long secure ID, the chance of a counterfeiter correctly guessing an ID used by a valid pharmaceutical manufacturer can be made arbitrarily small; e.g., 128-bit IDs, 192-bit IDs or even 256-bit IDs. Using this approach, RFID tags can all be manufactured in an identical way, eliminating security concerns at the IC foundry.

The secure RFID tag can be identified and authenticated using a secure challenge-response protocol as is used in many similar systems. The RFID reader first querries the tag, and the tag returns a unique ID number. The reader then uses that ID number to index into a secure database maintained by the pharmeceutical manufacturer or other trusted entity. The secure database returns a randomly selected challenge-response pair that is unique to the RFID and that is difficult/impossible to guess. The reader sends the challenge to tag. The tag generates the response and returns it to the reader. In this way it securely identifies itself, and the reader can authenticate the pharmeceutical from the secure database. Additional

information such as expiration date, dosage, type, etc. can be then securely read from the manufacturer's database.

There are a number of ways to generate secure challenge-response pairs. For our design, we plan to combine a secure shared key with a standard cryptographic function (in our case the commonly used 128b version of the Advanced Encryption Standard [8]). The key will be stored/generated using either an embedded non-volatile memory or a physical unclonable function (PUF). Either method is capable of storing/generating a key of sufficient length in a compact efficient manner. As performance is not critical in this application, we plan to use a compact serial implementation of AES as detailed below. The described system corresponds to a challenge-response system that uses a "strong" PUF built from a "weak" PUF combined with a known strong cryptographic function (AES). A counterfeiter could, in theory, read out the ID number from a number of genuine pills and clone them onto counterfeits, assuming they were able to reproduce the secure RFID tag design as well, requiring both pharmeceutical and IC cloning/counterfeiting capability. However, this would lead to multiple querries into the secure database from different readers, indicating that the tags had been cloned.

C. Cost

There are three components to the cost of secure RFID validation: the cost of the RFID tag, the cost of the RFID reader, and the support system cost. The corresponding cost constraints vary widely depending on the usage model. Every pill would have an RFID tag embedded within it. Thus, the cost of the RFID tags must be extremely low. The cost of the RFID reader should not be too expensive; i.e., it should not be burdensome for pharmacies, hospitals, clinics, etc. to purchase RFID readers. From the economic perspective of the pharmaceutical company, the cost of the RFID tags plus the cost of the server system, needs to be much smaller than the perceived cost savings due to reduction in counterfeiting.

Therefore, our primary focus is on lowering the cost of the RFID tags. Generally speaking, if we assume that the World Health Organization's estimate that 10% of all drugs worldwide are counterfeit, and that the proposed RFID solution could cut counterfeiting losses in half, then the savings is about 5% of revenue. For example, if the cost of the RFID Tag and the process of inserting it into a pill is on the order of 2% of the revenue associated with that pill or capsule, then an RFID tag solution makes sense. Using OCAs is important because it eliminates the cost of the antenna and the assembly cost, a dramatic cost savings for sub-mm^2 chips. Generally speaking, the cost of any IC is related to its die area and yield. Small dies generally have high yield, which reduces testing cost. Therefore, the primary goal is to make the IC die as small as possible to lower cost.

IV. Technology Building Blocks for Secure RFID

In this section we present the technology components that we propose to use to as building blocks for write-once secure RFID tags.

A. Secure Encryption Engine and ID Storage

The secure encryption engine and ID storage completely dominate the transistor count and power dissipation for the secure RFID tag. In order to maintain compatibility with existing encryption standards, we use the industry-standard AES algorithm with 128 bit IDs [8] and we note that AES use in RFID tags is well established; e.g., [5]. We have carried out significant development and design of advanced encryption standard (AES) engines, and of write-once programmable read only memory (PROM) units for ID storage; e.g., see Fig. 1. The major design/process challenge here is the reduction of power dissipation in the AES engine and ID storage.

We have designed a prototype RFID tag in a 65nm CMOS technology. The simulated performance of the AES engine and the ID memory, based on extracted layout are shown in Table 1. We have also carried out place and routing to generate the complete layout for this design as shown in Fig. 1.

	Area 65nm (μm^2)	**Power 1V, 500 MHz (mW)**	**Estimated Power 1V, 1MHz (μW)**
ID Store Memory	1,280	3.2	50
AES Crypto-Engine	13,500	5.1	443

TABLE 1: Performance estimate for ID store memory and AES Crypto-Engine.

With this design, operating at a 1V V_{DD}, the current drain is extrapolated to be 493μA at 1MHz clock frequency. The required current can be reduced to under 100μA by operating at a power supply voltage of 0.9V. Note, the total die area required in the 65nm process is about 120μm x 120μm for the AES engine and about 36μm x 36μm for the ID storage

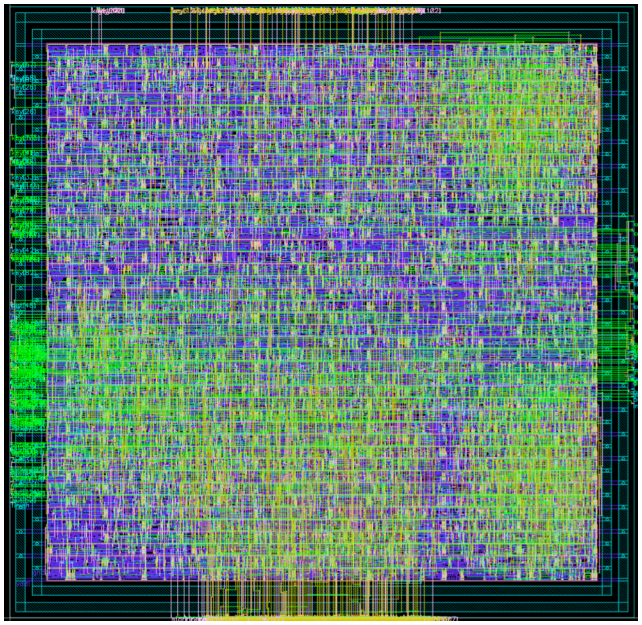

Fig. 1: Synthesized Layout of 128-bit AES engine.

memory. Although the size of these blocks could be reduced further by using a smaller feature-size CMOS technology, as will be shown below, the cost per unit area would increase and the overall integrated circuit die size would not decrease much because the die size will end up being dominated by the area required for the RF antenna.

B. RFID Power Harvesting Circuit

The RF circuitry must carry out three main subtasks: (i) efficiently rectifying and regulating the RF power received from the antenna, (ii) receiving communications data from the antenna in the form of amplitude-shift keying (ASK) modulation, and (iii) transmitting communications data to the antenna via antenna impedance shift keying. In this paper we focus on the first task, since harvesting RF power is extremely challenging given the small size of the tag antenna in this application and the other two steps are straightforward.

We adopt a standard approach for harvesting power from the incident RF signal using a balanced cross-coupled CMOS rectifier circuit [13][14], as shown in Fig. 2. This circuit is widely used in silicon CMOS passive RFID tags. In order to generate a 0.9V V_{DD} at the CMOS rectifier output, a roughly 1.3V peak-to-peak signal is required across the antenna terminals for the selected 65nm CMOS technology. In this design, the size of C_{Tag} must be chosen in order to make the tag antenna resonate at the desired operating frequency. Detailed operation of this CMOS RF rectifier is described in [14].

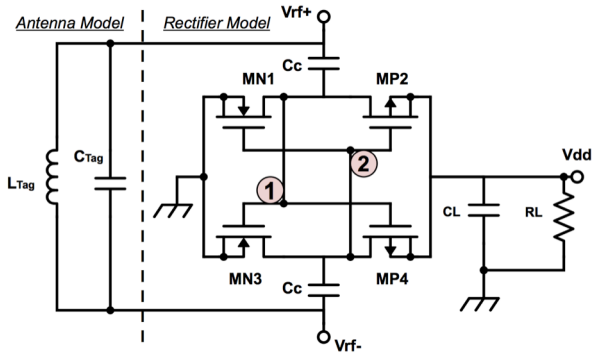

Fig. 2: Simplified schematic for RF rectifier circuit.

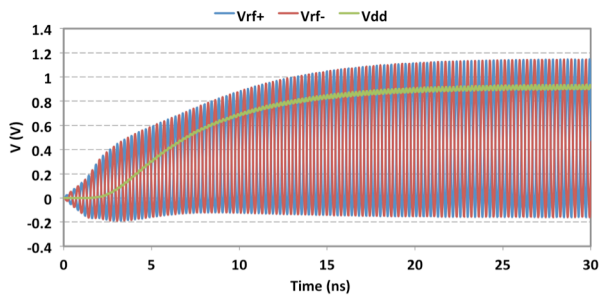

Fig. 3: Transient simulation of RF rectifier circuit showing steady state response to 64mVp-p induced voltage in tag antenna and with a 10kΩ resistive load for R_L.

In the selected 65nm CMOS process technology, the differential CMOS rectifier has a turn-on voltage of approximately 0.4Vp-p at the antenna terminals for either 2.4GHz or 5.8GHz signals. If a DC voltage of 0.9V is required in order to power the RFID tag circuitry modeled as a 10KΩ resistor, we need a peak-to-peak voltage induced in the 6.5nH antenna of at least 64mVp-p. This yields about 1.3Vp-p across the rectifier differential inputs at resonance and delivers 91μA of current to the resistive load at 0.9V; i.e., just over 80μW. The -3dB bandwidth around resonance is approximately 9.5% of the 2.45GHz center frequency indicating a loaded Q of about 10. Note, the Q drops as the RF input power increases.

C. RFID Tag Antenna and Reader-Tag Antenna Design

In this section we consider the design of the reader and tag antennas. First we consider the geometry of a medicinal pill authentication application. In its simplest form, the RFID reader consists of a loop antenna that is placed beside or around the pill. Since the typical diameter of pills and capsules is 10mm or less, we design for a working distance between the RFID tag and the RFID reader of up to 10mm, which is over 10X larger than that achieved in [3]. We have chosen to operate in the ISM band at 2.45GHz, which means that the distance between the RFID reader and the RFID tag is much less than a wavelength in free space (approximately 100mm at 2.45GHz). This geometry is refered to as inductively coupled. In such cases, the antenna system can be modeled as a loosely coupled transformer, as shown in Fig. 4.

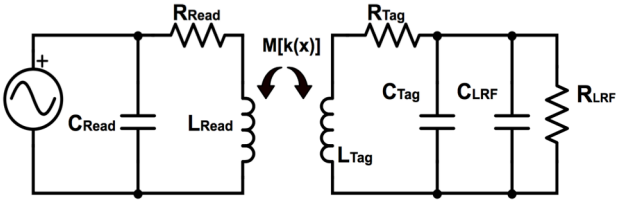

Fig. 4: Modeling the RFID reader antenna and the RFID tag antenna as coupled inductors.

In Fig. 4, the components on the left model the RFID reader and the components on the right model the RFID tag. The reader antenna is represented as L_{Read}, R_{Read}, and C_{Read}. We assume that the reader antenna has a current flowing through it of i_{Read}. The tag antenna is represented by L_{Tag}, R_{Tag}, and C_{Tag}. The input impedance of the aforementioned rectifier circuit, loaded by the RFID tag circuitry, are linearized for a given signal amplitude and approximated as R_{LRF} and C_{LRF}. C_{TOT}, C_{Tag} + C_{LRF}, can be increased with additional on-chip capacitance, if necessary, to tune the RFID tag resonance.

The design equation for inductively coupled RFID operation is well known. From [6], the voltage across R_{LRF} is

$$u_{Tag}(x) \approx \left(\frac{\omega\, k(x) \sqrt{L_{Tag} L_{Read}}\; i_{Read}}{\sqrt{\left(\omega \frac{L_{Tag}}{R_{LRF}} + \omega R_{Tag} C_{TOT}\right)^2 + \left(1 - \omega^2 L_{Tag} C_{TOT} + \frac{R_{Tag}}{R_{LRF}}\right)^2}} \right) \quad (1)$$

where $k(x)$ is the transformer coupling coefficient. $k(x)$ can be approximated as a function of just geometric terms [6]:

$$k(x) \approx \left(\frac{r_{Tag}\, r_{Read}}{x^2 + r_{Read}^2}\right)^{3/2} \quad (2)$$

In order to maximize the output voltage at the tag antenna, we choose to operate it at resonance, which makes the second term in the denominator of (1) go to zero. However, in order to address manufacturing variations, we choose to limit the loaded quality factor (Q) of the tag antenna resonant circuit to a value of at most 10. At resonance, the denominator can be recognized as the reciprocal of the loaded Q of the tag antenna, which we define as Q_{Tag} [7]. At resonance, we can simplify the equation for $u_{Tag}(x)$ as follows:

$$u_{Tag}(x) \approx k(x)\ \omega\ \sqrt{L_{Tag} L_{Read}}\quad i_{Read}\quad Q_{Tag} \quad (3)$$

The above equation can be used to determine the maximum working distance at which the 1.3V requirement set by the rectifier voltage input is satisfied.

We can estimate $k(x)$ by employing limitations that are imposed by the geometry. In particular, the RFID tag antenna radius, r_{Tag}, should be as large as possible to maximize the coupling coefficient. But, it is limited by the size of the chip. We observe that $k(x)$ does not depend the on the number of turns in either tag or reader antennas. Based on the size of the AES engine, and leaving additional room for the RF circuits and antenna, the die size is estimated to be about 0.3mm x 0.4mm. As will be shown below, this die size limits the antenna radius, r_{Tag}, to approximately 100µm. Initially, increasing the reader antenna radius, r_{Read}, increases $k(x)$, but once it is larger than the working distance, x, $k(x)$ decreases with further increases in r_{Read}. Therefore, we choose the radius of the RFID reader to be half of the maximum desired working distance; i.e., 5mm. Therefore, at an operating distance of x = 10mm, assuming r_{Tag} = 100µm and that r_{Read} = 5mm, k is approximately 0.026%. This extremely small coupling dramatically limits the power that can be transferred from the reader to the tag by inductive coupling.

For antennas in which the total length of the helix is short compared to its radius, which is approximately true in this case, the inductance of the antenna can be approximated as

$$L \approx N^2\ \mu_0\ r\ \ln\left(\frac{2r}{d}\right) \quad (4)$$

where N is the number of turns, r is the radius of the coil and d is the diameter of the wire [6]. Using the above equation and assuming N_{Read} = 1 and d_{Read} = 0.5mm, gives L_{Read} = 18.5nH. To deliver 200 µW of RF power, chosen to allow roughly 50% efficiency in the rectifier circuit, at 1.3Vp-p, requires $R_{LRF} \approx$ 1kΩ. For Q=10 at ω=2.45GHz, neglecting R_{Tag}, the inductance of L_{Tag} is 6.5nH. Ignoring R_{Tag} will be valid if Q of the antenna inductor alone is much higher than 10 at this frequency. Assuming that is true, the transimpedance from reader current to tag voltage is approximately 0.44Ω. To generate 1.3Vp-p at the tag will require about 3Ap-p flowing in the reader antenna. Because of the large diameter of the reader antenna wire, its Q can be very high, limited only by the necessary bandwidth required for the ASK modulation. And, there is no need to allow for manufacturing variations as the reader antenna can be tuned to the designed operating frequency at the time of manufacturing. Assuming reader Q=100, the reader antenna will dissipate just over 12W of power delivering 200µW of RF power to the tag antenna. Therfore, S_{21}=-48dB, which is only slightly worse than the theoretical best case coupling of -42dB (see *subsection D* below). Radiation resistance for the reader antenna is under 2Ω. The radiated power is under 2.5W, which is in compliance with ISM band device rules.

D. RFID Tag MEMS post-processing

In the previous subsection, we described the near-field inductive coupling between a reader antenna and a tag antenna in free space. However, the RFID tag OCA is adjacent to a conductive dielectric IC substrate. Using COMSOL [15] we simulated the best-case power transfer from the reader antenna to a 250µm diameter 1 turn tag antenna, for various tag antenna heights above a 0.4mm x 0.3mm x 0.3mm 10Ω-cm silicon substrate. The results are summarized in Fig. 5.

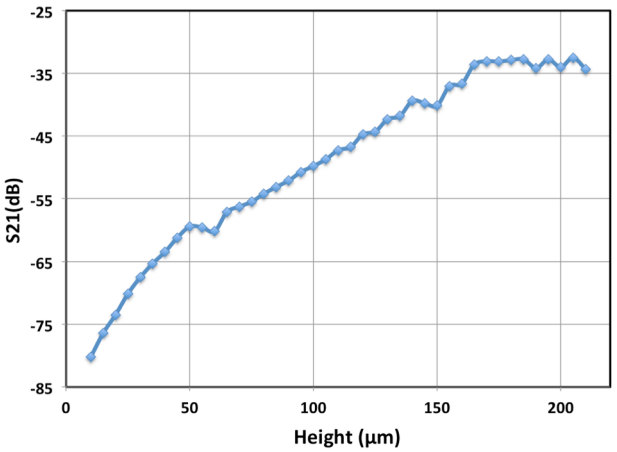

Fig. 5, Theoretical maximum power transfer from reader antenna to tag antenna vs height (in µm) of tag antenna above silicon substrate (optimal lossless power transfer).

Note that moving the antenna from the top of the metal stack for the IC up to anything above 180µm increases the power transfer from reader to tag antenna by 5 orders of magnitude. As can be seen in Fig. 5, the type of MEMS post-processing used in [3], raising the antenna an additional 15µm above the substrate, would gain less than 10dB. Unfortunately, the thick-film MEMS post-processing needed to raise the antenna by over 180µm is extremely challenging, which would dramatically decrease yield and increase cost. However, we also ran COMSOL simulations for the case of a loop antenna that was perpendicular to the silicon surface of the same geometry as before and found that the power transfer in that case was -42dB at 2.45GHz, which is equivalent to the power transfer to a tag antenna 140µm above the substrate and about 40dB (10,000X) higher than to the coil right on to of the IC.

In this paper, we propose the use of an out of plane helical antenna coil that makes use of a novel low-cost MEMS fabrication method. We have fabricated such coils in the CMU Nanofabrication facility; e.g., Fig. 6. In the 1980's, Xerox PARC first proposed using self assembly for inductors and this work was extended at Xerox [16] and Purdue [17]. Our approach to building vertical, out-of-plane antennas starts by patterning a metal bilayer that incorporates a large stress difference on top of a sacrificial layer. The original location of the coil turns can be seen as shadowed areas in Fig. 6. When the sacrificial layer is removed using a gas-phase etch, the two metal bilayer beams each curl out of plane toward the middle.

A tongue and groove structure causes the two sides to meet and lock together, as shown in Fig. 6. This assembly is then electroplated with approximately 2μm of copper permanently joining the tips of the beams, strengthening the structure and reducing its series resistance. Finally, a thick inert passivation layer is deposited on top of the wafer and cured, protecting the coil from handling and keeping the human from being exposed to the coil materials. The advantage of the proposed approach over just raising the antenna above the substrate is that it only requires depositing and patterning thin films. The 3D aspect of the structure is created by self-assembly and no patterning is required in the thick passivation layer added at the end. These keep the additional fabrication costs low, resulting in an extremely low cost for the final RFID tag.

Assuming the plated diameter of the coil windings is approximately 5μm and r_{Tag} = 100μm, we select N_{Read} to be 4. Since the antenna is center-tapped, there are 2 turns on each side of the center tap. Applying eqn (4), gives an inductance for the Tag antenna of approximately L_{Tag} = 7.4nH, which is as close as can be achieved to 6.5nH with an even integer N_{Read}.

V. Conclusions

In this paper a concept for secure authentication of mecidines in the form of pills and capsules using secure RFID tags embedded into the medicines has been presented. Analysis results were presented that indicate the 10mm working range, more than 10X that of similar prior work, is achievable using the novel perpendicular helical antenna structure described herein. E&M simulation results were presented assessing the impact of various antenna structures on power transfer from the reader to the tag. Proof-of-concept helical antenna structures have been fabricated and presented, thereby demonstrating the feasibility of the low-cost MEMS approach to their fabrication.

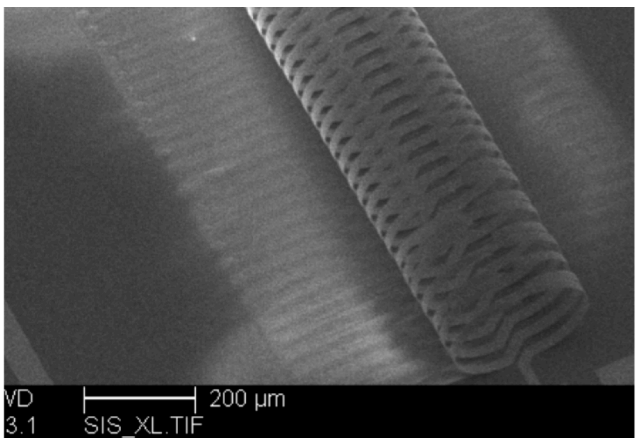

Fig. 6: MEMS fabricated self-assembled out-of plane helical antenna structure before plating with copper.

Acknowledgment

We would like to thanks ST Microelectronics for providing access to their 65nm CMOS integrated circuit foundry process and Peregine Semiconductor for providing access to their 130nm RF CMOS SOI process.

References

[1] Abrial André, Jacky Bouvier, Marc Renaudin, Patrice Senn and Pascal Vivet., "A new contactless smart card IC using an on-chip antenna and an asynchronous microcontroller," *IEEE J. Solid-State Circuits*, vol. 36, no. 7, pp. 1101–1107, Jul. 2001.

[2] M. Usami, "An ultra small RFID chip: μ-chip," in *IEEE RFIC Symp. Dig.*, pp. 241–244, Jun. 2004.

[3] Chen Xuesong, Wooi Gan Yeoh, Yeung Bun Choi, Hongyu Li, and Rajinder Singh, "A 2.45-GHz Near-Field RFID System With Passive On-Chip Antenna Tags," in *IEEE Transactions on Microwave Theory and Techniques*, vol. 56, no. 6, June 2008.

[4] http://www.proteus.com/press-releases/u-s-fda-accepts-first-digital-medicine-new-drug-application-for-otsuka-and-proteus-digital-health/.

[5] Man, A.S.W., E. S. Zhang, V. K. N. Lau, C. Y. Tsui and H. C. Luong, "Low Power VLSI Design for a RFID Passive Tag baseband System Enhanced with an AES Cryptography Engine," *RFID Eurasia*, 2007 1st Annual, Istanbul, 2007, pp. 1-6.

[6] Finkenzeller, K., RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 2nd ed. New York: Wiley, 2003.

[7] Lee, T.S., The Design of CMOS Radio-Frequency Integrated Circuits, 2nd Edition, Cambridge University Press, New York, 2004.

[8] Federal Information Processing Standards, vol. 197, 2001.

[9] Scherjon, Cor, "RFID Transponders," Chapter 30 in Ultra-thin Chip Technology and Applications, Burghartz, J.N. (ed.), pp. 389-398, Springer Science+Business Media, LLC 2011.

[10] Jingtian X., Y. Na, C. Wenyi, X. Conghui, W. Ciao, Y. Yuqing, J. Hongyan, and M. Hau, "Lowcost low-power UHF RFID tag with on-chip antenna." J. Semiconductors, 30(7):1–6, 2009.

[11] Datz, T. "Drugmakers Testing RFID Tags: Counterfeit drugs are as common as a knockoff Hermès tie or Prada bag on the streets of Manhattan,", http://www.csoonline.com/article/2118948/supply-chain-security/drugmakers-testing-rfid-tags.html, CSO Media, 1 Nov 2005.

[12] Radiom S, De Roover C, Vandenbosch G, Steyaert M, and G. Gielen, "A Fully integrated pinless long-range power supply with on-chip antenna for scavenging-based rfid tag powering, silicon monolithic integrated circuits in RF systems," SiRF 2009. IEEE Topical Meeting, pp. 1–4, Jan 2009.

[13] Facen A. and A. Boni, "Power supply generation in CMOS passive UHF RFID tags," Research in Microelectronics and Electronics, pp. 33–36, 2006.

[14] Mandal S. and R. Sarpeshkar, "Low-power CMOS rectifier design for RFID applications," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 54, no. 6, pp. 1177 –1188, Jun. 2007.

[15] Comsol Multiphysics, www.comsol.com.

[16] Chua, C.L., D. K. Fork, K. Van Schuylenbergh, and J.-P. Lu, "Out-of-Plane High-Q Inductors on Low-Resistance Silicon," J. Micro-electromechanical Systems, Vol. 12, No. 6, pp. 989-995. Dec. 2003.

[17] Weon D.-H., J.-H. Jeong, and S. Mohammadi, "High-Q micromachined three-dimensional integrated inductors for high-frequency applications," J. Vac. Sci. Technol. B vol. 25, no. 1, Jan/Feb 2007.